

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, James V. Richardson, being duly sworn, depose and state as follows:

INTRODUCTION

1. I am a Special Agent with United States Department of Homeland Security (DHS), Immigrations and Customs Enforcement (ICE), Homeland Security Investigations (HSI), and am assigned to the office of the Resident Agent in Charge, Providence, RI. I have been an agent of HSI since 2009. As part of my duties, I am authorized to investigate violations of the laws of the United States, including criminal violations relating to child exploitation, child pornography, coercion and enticement, and transportation of minors, and the transfer of obscene material to minors, including but not limited to, violations of 18 U.S.C. §§ 2251, 2252, and 2252A. I have received training in the investigation of child pornography, child exploitation, and transportation of minors, and have had the opportunity to observe and review examples of child pornography (as defined in 18 U.S.C. § 2256).

2. I am currently participating in an investigation relating to violations of federal law by Eugenio GOMES (DOB XX/XX/1977) for possession of child pornography, in violation of 18 U.S.C. § 2252(a)(4)(B). I submit this affidavit in support of applications to search:

- a. the person of Eugenio GOMES, date of birth XX/XX/1977 (hereinafter “GOMES” and/or the “SUBJECT PERSON”),
- b. GOMES’s residence, the premises located at 54 Seabiscuit Place, Pawtucket, RI 02861 (the “SUBJECT PREMISES”),
- c. contents of the Verizon cloud storage account associated with telephone number 401-450-9792 (the “TARGET ACCOUNT”),

and the content of any electronic media storage devices or media located on the SUBJECT PERSON or in the SUBJECT PREMISES, as more fully described in Attachments A-1, A-2 and A-3, which are incorporated herein by reference; and to seize evidence, instrumentalities, fruits of crime, and contraband as more fully described in Attachments B-1, B-2 and B-3, which are also incorporated herein by reference.

PROBABLE CAUSE AND BACKGROUND OF THE INVESTIGATION

3. In August 2023, I reviewed a report from the National Center for Missing and Exploited Children (NCMEC)¹ regarding a subject uploading and possessing child sexual abuse material (CSAM). The NCMEC received information from Synchronoss Technologies Inc. (Synchronoss²) regarding a Verizon subscriber utilizing telephone number 401-450-9792 who uploaded 7 CSAM files to their Verizon cloud account. The NCMEC also reported an additional nine (9) reports for the same phone number with 63 additional CSAM files reported as uploaded to the Verizon cloud account. I reviewed the CSAM files provided by Synchronoss and confirmed its content to be consistent with the definition of child pornography as defined in 18 U.S.C. § 2256.

4. The following are examples of CSAM files possessed by Verizon subscriber 401-450-9792:

File name:

ba0bc279c505409eb42c5bc7722fd335_61eaa6cf0552d2695b68f37b17c78c6a936
be49ecbb361b437f7b3472dfa9d27.jpg

Description: This image file depicts a nude prepubescent female lying on her back with her legs spread apart, exposing her vagina in a lascivious manner.

File name:

ba0bc279c505409eb42c5bc7722fd335_1202f132fcffdf07a90fe860f1ac9ea7425d8
803d4e3d95d65cc70c396eba095.jpg

Description: This image file depicts a nude prepubescent female on her knees in a bent position, exposing her vagina and anus in a lascivious manner.

¹ The NCMEC is a nonprofit organization that provides services nationwide for families and professionals in the prevention of abducted, endangered, and sexually exploited children. Pursuant to its mission and its congressional authorization, the NCMEC operates a CyberTipline to assist law enforcement in identifying victims of child pornography and child exploitation and works with law enforcement to reduce the distribution of child exploitation images and videos over the Internet.

² According to the Cybertip, Synchronoss Technologies is the cloud-based storage provider on the Verizon Cloud. According to the online Verizon User Guide, a cloud user can access his or her content through the My Verizon website or the Verizon Cloud app on his or her Apple® iOS device, Android™ device or computer (Windows® or Mac®).

File name:

ba0bc279c505409eb42c5bc7722fd335_7ec1446325d9567faab8dc5c3a8380e2815
b6d491f2b650a010ed781db46f9a0.jpg

Description: This image file depicts a nude prepubescent female with semen on her face, neck and chest.

5. Using a commercial database, I queried telephone number 401-450-9792. The results of the query show that telephone number belonging to Eugenio GOMES (DOB XX/XX/1977). I then used the same commercial database to query Eugenio GOMES with a date of birth of XX/XX/1977. The following are the results of that query:

Name: Eugenio GOMES

Address: 54 Seabiscuit Place, Pawtucket, RI 02861

DOB: XX/XX/1977 (Age 46)

SSN: 038-52-2773

6. On August 11, 2023, I queried the Rhode Island Division of Motor Vehicles (DMV) using the name Eugenio GOMES with the same date of birth as above. The RI DMV returned the following information:

Name: Eugenio GOMES

DOB: XX/XX/1977

Eye color: brown

Height: 5'05"

Weight: 166

Gender: male

SSN: 038-52-2773

Address: 54 Seabiscuit Place, Pawtucket, RI 02861

Driver ID: 9316190

Issue date: 2021-06-13

Expiration date: 2026-05-27

Status: Valid

7. On September 21, 2023, I sent legal process to Verizon Wireless requesting subscriber information for telephone number 401-450-9792. On September 28, 2023, Verizon responded with the following information:

Name: Eugenio GOMES

Address: 54 Seabiscuit Place, Pawtucket, RI 02861

Account Number: 381559021-1

MTN Effective Date: 09/20/2006

8. I queried a commercial database for 54 Seabiscuit Place, Pawtucket, RI 02861, and it appears two individuals are residing at the SUBJECT PREMISES: Eugenio GOMES (DOB 1977) and Carla GOMES (DOB 1976).

9. On September 25, 2023, the United States Postal Service (USPS) confirmed that both Eugenio GOMES and Carla GOMES are currently receiving mail at the SUBJECT PREMISES. On September 25, 2023, physical surveillance was conducted at the SUBJECT PREMISES. The SUBJECT PREMISES observed was a tan, one-story, ranch-style, single family home. The number "54" is clearly affixed to the house to the left of the front door. In the driveway to the right of the house, two vehicles with RI registrations were observed. I queried the Rhode Island Department of Motor Vehicles for registration SP306 and learned that the vehicle is registered to Maria G. Gomes, 54 Seabiscuit Place, Pawtucket, RI 02861. I queried the Rhode Island Department of Motor Vehicles for registration 46538 and learned that the vehicle is registered to Franco Enterprises, Inc, 194 Waterman Street, Suite 1B, Providence, RI 02906. In 2008, Eugenio GOMES was encountered by the Little Compton Police Department via a traffic stop. GOMES was driving a company vehicle at the time and listed his employer as Franco Enterprises.

**CHARACTERISTICS COMMON TO PERSONS WHO ENGAGE IN
CHILD SEXUAL EXPLOITATION**

10. Based on my previous investigative experience related to child exploitation investigations, and the training and experience of other law enforcement officers with whom I have collaborated, I have learned that there are certain characteristics that are generally common to offenders who access, send, distribute, exhibit, possess, display, transport, manufacture, or produce material which depicts minors engaged in sexually explicit conduct, or who engage in sexually explicit communications with minors. Said material includes, but is not limited to, photographs and videos stored electronically on computers, digital devices, or related digital storage media.

11. Such offenders may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have that stem from viewing children engaged

in sexual activity or in sexually suggestive poses, whether in person, in photographs or other visual media, or from literature describing such activity.

12. Such offenders may collect sexually explicit or suggestive materials in a variety of media, including digital photographs, videos, or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to facilitate contact offenses – that is, to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

13. Such offenders almost always possess and maintain their hard copies of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain their cache for many years. In my training and experience, I am aware that such offenders often keep copies of their CSAM collections even if they move from one residence to another or change electronic media devices such as their smart phone or tablet.

14. Likewise, such individuals often maintain their child pornography images in a digital or electronic format in a safe, secure, and private environment, such as a “SD card,” computer or surrounding area. These child pornography images are often maintained for several years and are kept close by, usually at the offender’s residence, inside the offender’s vehicle, or, at times, on his person, to enable the individual to view the child pornography images, which are highly valued.³

15. Some of these individuals, however, have been found to download, view, and then delete child pornography on their computers or digital devices on a cyclical and repetitive basis, presumably to avoid criminal liability. Importantly, as described in more detail below, evidence of such activity, including deleted child pornography, often can be located on these individuals’ computers and digital devices through the use of forensic tools. Indeed, the very nature of electronic storage means that evidence of the crime is often still discoverable for extended periods

³ See *United States v. Morales-Aldahondo*, 524 F.3d 115, 117-119 (1st Cir. 2008) (3-year delay between last download and warrant application not too long, given affiant testimony that consumers of child pornography value collections and thus often retain them for a period of time, and consumers who use computers to access child pornography are likely to use computers to store their collections).

of time even after the individual “deleted” it.⁴

16. Such offenders also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/possessors, conceal such correspondence as they do their sexually explicit material, and often maintain lists or other record of individuals with whom they have been in contact and who share the same interests in child pornography.

17. Such offenders prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world. Thus, even if such an offender uses a portable device (such as a mobile phone or gaming device) to access the internet and child pornography, it is more likely than not that evidence of this access will be found in his home – here, the SUBJECT PREMISES, as set forth in Attachment A-2.

18. Based upon the foregoing, I believe that Eugenio GOMES likely displays characteristics common to individuals who access with the intent to view and possess, collect, receive, or distribute child pornography. As such, I submit that there is probable cause to believe that contraband material depicting minors engaged in sexually explicit conduct and other evidence, instrumentalities, and fruits of violations of possession of child pornography, in violation of 18 U.S.C. § 2252(a)(4)(B) exist at the SUBJECT PREMISES.

SEARCH AND SEIZURE OF COMPUTER SYSTEMS AND DATA

19. Based on my knowledge, training, experience, and information provided to me by other agents, I know that computer files or remnants of such files can be recovered months or even years after they have been written, downloaded, saved, deleted, or viewed locally or over the Internet. This is true because:

a. Electronic files that have been downloaded to a storage medium can be stored for years at little or no cost. Furthermore, when users replace their computers, they can easily transfer the data from an old computer to a new computer.

b. Even after files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium

⁴ See *United States v. Seiver*, 692 F.3d 774, 775-776 (7th Cir. 2012) (in context of staleness challenge, collecting and agreeing with cases from the 4th, 5th, 6th, and 9th Circuits that acknowledge the ability of forensic examiners to recover evidence of child pornography even after such files are deleted by a user).

until it is overwritten by new data, which might not occur for long periods of time. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media – in particular, computers' internal hard drives – contain electronic evidence of how the computer has been used, what it has been used for, and who has used it. This evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. It is technically possible to delete this information, but computer users typically do not erase or delete this evidence because special software is usually required for that task.

d. Similarly, files that have been viewed over the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache." The browser often maintains a fixed amount of hard drive space devoted to these files, and the files are overwritten only as they are replaced with more recently viewed Internet pages or if a user takes steps to delete them.

20. Based on my knowledge and training and the experience of other agents with whom I have spoken, I am aware that in order to completely and accurately retrieve data maintained in computer hardware, computer software, or storage media, to ensure the accuracy and completeness of such data, and to prevent the loss of the data either from accidental or programmed destruction, it is often necessary that computer hardware, computer software, computer-related documentation, and storage media ("computer equipment") be seized and subsequently processed by a qualified computer specialist in a laboratory setting, rather than in the location where it is seized. This is true because of:

a. The volume of evidence: Storage media such as hard disks, SD cards, flash drives, CD-ROMs, and DVD-ROMs can store the equivalent of thousands or, in some instances, millions of pages of information. Additionally, a user may seek to conceal evidence by storing it in random order or with deceptive file names. Searching authorities may need to examine all the stored data to determine what particular files are evidence, fruits, or instrumentalities of criminal activity. This process can take weeks or months, depending on the volume of data stored, and it would be impractical to attempt this analysis on-site.

b. Technical requirements: Analyzing computer hardware, computer software, or storage media for criminal evidence is a highly technical process requiring expertise and a properly controlled environment. The vast array of computer hardware and software available requires

even computer experts to specialize in some systems and applications. Thus, it is difficult to know, before the search, which expert possesses sufficient specialized skill to best analyze the system and its data. Furthermore, data analysis protocols are exacting procedures, designed to protect the integrity of the evidence and to recover even “hidden,” deleted, compressed, password-protected, or encrypted files. Many commercial computer software programs also save data in unique formats that are not conducive to standard data searches. Additionally, computer evidence is extremely vulnerable to tampering or destruction, both from external sources and destructive code imbedded in the system as a “booby trap.”

BIOMETRIC ACCESS TO DEVICES

21. This warrant permits law enforcement to compel Eugenio GOMES to unlock any DEVICES requiring biometric access subject to seizure pursuant to this warrant. The grounds for this request are as follows:

- a. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.
- b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called “Touch ID,” which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device’s Touch ID sensor, which is found in the round button (often referred to as the “home” button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.
- c. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is

available on certain Android devices and is called “Trusted Face.” During the Trusted Face registration process, the user holds the device in front of his or her face. The device’s front-facing camera then analyzes, and records data based on the user’s facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Trusted Face.

- d. If a device is equipped with an iris-recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called “Windows Hello.” During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user’s face and activates an infrared-sensitive camera to record data based on patterns within the user’s irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris-recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.
- e. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device’s contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.
- f. As discussed in this Affidavit, your Affiant has reason to believe that one or more digital devices will be found during the search. The passcode or password that would unlock the DEVICES subject to search under this warrant currently is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the DEVICES, making the use of biometric features necessary to the execution of the search authorized by this warrant.

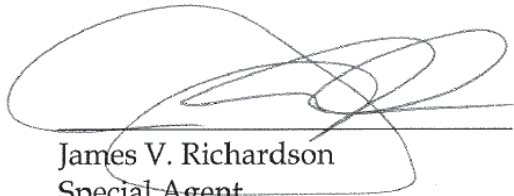
- g. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when: (1) more than 48 hours has elapsed since the device was last unlocked; or (2) when the device has not been unlocked using a fingerprint for 8 hours *and* the passcode or password has not been entered in the last 6 days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.
- h. Due to the foregoing, if law enforcement personnel encounter any DEVICES for which they have a reasonable belief belong to GOMES that are subject to seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, this warrant permits law enforcement personnel to: (1) press or swipe the fingers (including thumbs) of Eugenio GOMES to the fingerprint scanner of the DEVICES found at the premises; (2) hold the DEVICES found at the premises in front of the face of Eugenio GOMES and activate the facial recognition feature; and/or (3) hold the DEVICES found at the premises in front of the face of Eugenio GOMES and activate the iris recognition feature, for the purpose of attempting to unlock the DEVICES in order to search the contents as authorized by this warrant. The proposed warrant does not authorize law enforcement to compel that Eugenio GOMES state or otherwise provide the password or any other means that may be used to unlock or access the DEVICES. Moreover, the proposed warrant does not authorize law enforcement to compel Eugenio GOMES to identify the specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the DEVICES.

CONCLUSION

22. Based on the foregoing, there is probable cause to believe that the federal criminal statutes cited herein have been violated, and that the contraband, property, evidence, fruits and instrumentalities of these offenses, more fully described in Attachment B-1, Attachment B-2 and Attachment B-3, are located on the person, at the locations, and in the accounts described in Attachment A-1, Attachment A-2 and Attachment A-3. I respectfully request that this Court issue search warrants for the person, location and accounts described in Attachment A-1, Attachment A-2 and Attachment A-3, authorizing the seizure and search of the items described in Attachment B-1, Attachment B-2 and Attachment B-3 respectively.

23. I am aware that the recovery of data by a computer forensic analyst takes significant time; much the way recovery of narcotics must later be forensically evaluated in a lab, digital evidence will also undergo a similar process. For this reason, the “return” inventory will contain a list of only the tangible items recovered from the premises. Unless otherwise ordered by the Court, the return will not include evidence later examined by a forensic analyst.

Sworn to under the pains and penalties of perjury,


James V. Richardson
Special Agent
Homeland Security

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by:

telephone _____
(specify reliable electronic means)

Date

Providence, Rhode Island
City and State

Judge's signature

Lincoln D. Almond, US Magistrate Judge
Printed name and title

ATTACHMENT A-1

DESCRIPTION OF PERSON TO BE SEARCHED

The person of Eugenio GOMES, a male, standing approximately 5'05", date of birth XX/XX/1977 (the SUBJECT PERSON).



The search shall include the content of any electronic media storage devices, including smart phones, or media located on the person of Eugenio GOMES, regardless of the location at which he may be found.

ATTACHMENT B-1
DESCRIPTION OF INFORMATION TO BE SEIZED⁵

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use, or which is or has been used as the means of committing a criminal offense, namely violations of 18 U.S.C. § 2252(a)(4)(B) and 18 U.S.C. § 2252(a)(2):

1. Computers or storage media used as a means to commit the violations described above.
2. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which are stored records or information that is otherwise called for by this warrant (hereinafter, “COMPUTER”):

⁵ For the purpose of this warrant, and attachments thereto:

A. “Records” and “information” may be any collection of data or information, including communications. A record may be comprised of letters, numbers, pictures, sounds or symbols. Records and information include all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

B. “Computer” includes all types of electronic, magnetic, optical, electrochemical, or other high-speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

C. “Computer equipment” means any computer hardware, computer software, computer-related documentation, storage media, and data.

D. “Computer hardware” means any electronic device capable of data processing (such as a computer, gaming device, smartphone, cellular telephone, or wireless communication device); any peripheral input/output device (such as a keyboard, printer, scanner, monitor, and drive intended for removable storage media); any related communication device (such as a router, wireless card, modem, cable, and any connections), and any security device, (such as electronic data security hardware and physical locks and keys).

E. “Computer software” means any program, program code, information or data stored in any form (such as an operating system, application, utility, communication and data security software; a log, history or backup file; an encryption code; a username; or a password), whether stored deliberately, inadvertently, or automatically.

F. “Computer related documentation” means any material that explains or illustrates the configuration or use of any seized computer hardware, software, or related items.

G. “Data” means all information stored on storage media of any form in any storage format and for any purpose.

H. “Storage medium” and/or “storage media” includes any physical object upon which computer data can be recorded, collected, retrieved, and/or transmitted, including external and internal hard drives, flash drives, thumb drives, micro-SD cards, macro-SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact discs, DVDs, magnetic tapes, memory cards, memory chips, and other magnetic or optical media.

I. “Obscene material” is any image or video representation containing material which the average person, applying contemporary community standards would find that the work, taken as a whole, appeals to the prurient interest; depicts in a patently offensive way, sexual conduct and taken as a whole, lacks serious literary, artistic, political, or scientific value such as patently offensive representations or descriptions of ultimate sexual acts, normal or perverted, actual or simulated, patently offensive representation or descriptions of masturbation, excretory functions, and lewd exhibition of the genitals.

- a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, and correspondence;
- b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- c. evidence of the lack of such malicious software;
- d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to the crime(s) under investigation and to the computer user;
- e. evidence indicating the computer user’s knowledge and/or intent as it relates to the crime(s) under investigation;
- f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- g. evidence of programs (and associated data) that are designed to eliminate data from the COMPUTER;
- h. evidence of the times the COMPUTER was used;
- i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- k. records of or information about Internet Protocol addresses used by the COMPUTER;
- l. records of or information about the COMPUTER’s Internet activity, including firewall logs, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and
- m. contextual information necessary to understand the evidence described in this

attachment.

3. Routers, modems, and network equipment used to connect computers to the Internet.
4. Child pornography, as defined in 18 U.S.C. § 2256(8), visual depictions of minors engaging in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2), and child erotica.
5. Records, information, and items relating to violations of the statutes described above including:
 - a. Records, information, and items relating to the occupancy or ownership of the 54 Seabiscuit Place, Pawtucket, RI 02861 (SUBJECT PREMISES), including utility and telephone bills, mail envelopes, or addressed correspondence;
 - b. Records, information, and items relating to the ownership or use of computer equipment found in the SUBJECT PREMISES, including sales receipts, bills for Internet access, and handwritten notes;
 - c. Records and information relating to the identity or location of the persons suspected of violating the statutes described above;
 - d. Records and information relating to sexual exploitation of children, including correspondence and communications between users of child pornography and exploitation websites.

During the execution of the search of the SUBJECT PERSON described in Attachment A-1 and the SUBJECT PREMISES described in Attachment A-2, law enforcement personnel are also specifically authorized to compel the SUBJECT PERSON, Eugenio GOMES, to provide biometric features, including pressing fingers (including thumbs) against and/or putting a face before the sensor, or any other security feature requiring biometric recognition, of:

- (a) any of the DEVICES found on the SUBJECT PERSON and any of the DEVICES found at the SUBJECT PREMISES for which they have a reasonable belief belong to GOMES, and
- (b) where the DEVICES are limited to those which are capable of containing and reasonably could contain fruits, evidence, information, contraband, or instrumentalities of the offense(s) as described in the search warrant affidavit and warrant attachments,

for the purpose of attempting to unlock the DEVICES' security features in order to search the

contents as authorized by this warrant.

This warrant does not authorize law enforcement personnel to compel any other individuals found at the SUBJECT PREMISES to provide biometric features, as described in the preceding paragraph, to access or otherwise unlock any DEVICE. Further, this warrant does not authorize law enforcement personnel to request that Eugenio GOMES to state or otherwise provide the password or any other means that may be used to unlock or access the DEVICES, including by identifying the specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the DEVICES.

ATTACHMENT A-2

DESCRIPTION OF LOCATION TO BE SEARCHED

The premises to be searched include:

The Premises located at 54 Seabiscuit Place, Pawtucket, RI 02861, more particularly described as a tan, one-story, ranch-style, single family home. The number “54” is clearly affixed to the house to the left of the front door. The exterior of the premises is pictured below:



ATTACHMENT B-2

DESCRIPTION OF INFORMATION TO BE SEIZED⁶

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of 18 U.S.C. § 2252(a)(4)(B) and 18 U.S.C. § 2252(a)(2):

1. Computers or storage media used as a means to commit the violations described above.
2. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which are stored records or

⁶ For the purpose of this warrant, and attachments thereto:

A. "Records" and "information" may be any collection of data or information, including communications. A record may be comprised of letters, numbers, pictures, sounds or symbols. Records and information include all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

B. "Computer" includes all types of electronic, magnetic, optical, electrochemical, or other high-speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

C. "Computer equipment" means any computer hardware, computer software, computer-related documentation, storage media, and data.

D. "Computer hardware" means any electronic device capable of data processing (such as a computer, gaming device, smartphone, cellular telephone, or wireless communication device); any peripheral input/output device (such as a keyboard, printer, scanner, monitor, and drive intended for removable storage media); any related communication device (such as a router, wireless card, modem, cable, and any connections), and any security device, (such as electronic data security hardware and physical locks and keys).

E. "Computer software" means any program, program code, information or data stored in any form (such as an operating system, application, utility, communication and data security software; a log, history or backup file; an encryption code; a username; or a password), whether stored deliberately, inadvertently, or automatically.

F. "Computer related documentation" means any material that explains or illustrates the configuration or use of any seized computer hardware, software, or related items.

G. "Data" means all information stored on storage media of any form in any storage format and for any purpose.

H. "Storage medium" and/or "storage media" includes any physical object upon which computer data can be recorded, collected, retrieved, and/or transmitted, including external and internal hard drives, flash drives, thumb drives, micro-SD cards, macro-SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact discs, DVDs, magnetic tapes, memory cards, memory chips, and other magnetic or optical media.

I. "Obscene material" is any image or video representation containing material which the average person, applying contemporary community standards would find that the work, taken as a whole, appeals to the prurient interest; depicts in a patently offensive way, sexual conduct and taken as a whole, lacks serious literary, artistic, political, or scientific value such as patently offensive representations or descriptions of ultimate sexual acts, normal or perverted, actual or simulated, patently offensive representation or descriptions of masturbation, excretory functions, and lewd exhibition of the genitals.

information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

- a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
- b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- c. evidence of the lack of such malicious software;
- d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to the crime(s) under investigation and to the computer user;
- e. evidence indicating the computer user's knowledge and/or intent as it relates to the crime(s) under investigation;
- f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- g. evidence of programs (and associated data) that are designed to eliminate data from the COMPUTER;
- h. evidence of the times the COMPUTER was used;
- i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- k. records of or information about Internet Protocol addresses used by the COMPUTER;
- l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and

- m. contextual information necessary to understand the evidence described in this attachment.
- 3. Routers, modems, and network equipment used to connect computers to the Internet.
- 4. Child pornography, as defined in 18 U.S.C. § 2256(8), visual depictions of minors engaging in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2), and child erotica.
- 5. Records, information, and items relating to violations of the statutes described above including:
 - a. Records, information, and items relating to the occupancy or ownership of the SUBJECT PREMISES, including utility and telephone bills, mail envelopes, or addressed correspondence;
 - b. Records, information, and items relating to the ownership or use of computer equipment found in the SUBJECT PREMISES, including sales receipts, bills for Internet access, and handwritten notes;
 - c. Records and information relating to the identity or location of the persons suspected of violating the statutes described above;
 - d. Records and information relating to sexual exploitation of children, including correspondence and communications between users of child pornography and exploitation websites.

During the execution of the search of the SUBJECT PREMISES described in Attachment A-2, law enforcement personnel are also specifically authorized to compel the SUBJECT PERSON, Eugenio GOMES, to provide biometric features, including pressing fingers (including thumbs) against and/or putting a face before the sensor, or any other security feature requiring biometric recognition, of:

- (a) any of the DEVICES found on the SUBJECT PERSON and any of the DEVICES found at the SUBJECT PREMISES for which they have a reasonable belief belong to GOMES, and
- (b) where the DEVICES are limited to those which are capable of containing and reasonably could contain fruits, evidence, information, contraband, or instrumentalities of the offense(s) as described in the search warrant affidavit and warrant attachments,

for the purpose of attempting to unlock the DEVICES' security features in order to search the contents as authorized by this warrant.

This warrant does not authorize law enforcement personnel to compel any other individuals found at the SUBJECT PREMISES to provide biometric features, as described in the preceding paragraph, to access or otherwise unlock any DEVICE. Further, this warrant does not authorize law enforcement personnel to request that Eugenio GOMES to state or otherwise provide the password or any other means that may be used to unlock or access the DEVICES, including by identifying the specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the DEVICES.

ATTACHMENT A-3

DESCRIPTION OF ACCOUNT TO BE SEARCHED

This warrant applies to information associated with the Verizon cloud account for telephone number 401-450-9792 that is stored at premises owned, maintained, controlled, or operated by Synchronoss Technologies, Inc., a company located at 200 Crossing Blvd., Bridgewater, NJ 08807.

ATTACHMENT B-3
DESCRIPTION OF INFORMATION TO BE SEIZED

I. Information to be disclosed by Synchronoss Technologies, Inc.:

To the extent that the information described in Attachment A-3 is within the possession, custody, or control of Synchronoss Technologies Inc., including any messages, records, files, logs, or information that have been deleted but are still available to Synchronoss Technologies Inc., or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Google is required to disclose the following information to the government for each account or identifier listed in Attachment A-3:

- a. Any communications involving the users of each account or identifier listed in Attachment A-3.
- b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
- c. The types of service utilized by the user;
- d. All records or other information stored by an individual using the account, including communications, photographs, images and videos;
- e. All records pertaining to communications between Synchronoss Technologies Inc. and any person regarding the account, including contacts with support services and records of actions taken.

II. Information to be seized by the government:

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of 18 U.S.C. §§ 2252 involving Eugenio GOMES, including, for each account or identifier listed on Attachment A-3 for the time period specified, information pertaining to the following matters:

- a. Any communications, including any photographs, images, videos or other attachments, between the users of the accounts or identifiers listed on Attachment A-3 and others regarding the distribution, receipt or possession, or attempt to do so, of child pornography.
- b. Evidence indicating how and when the account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner.
- c. The identities of the persons who created or used the accounts or identifiers listed in Attachment A-3, including records that help reveal the whereabouts of such persons.

The identities of the persons who communicated with the users of the accounts or identifiers listed in Attachment A-3 about matters relating to the distribution, receipt, or possession of child pornography, including records that help reveal their whereabouts.